



Operator's Startup Guide

for use with ...
Cyfin and CyBlock Web-use Monitoring Products

Wavecrest Computing, Inc.

Operator's Startup Guide

Table of Contents

Preface

Section 1. Introduction

Section 2. Your Product's Reporting Capability: an Overview

Section 3. Your Operator Account

Section 4. First-Time Report Generation

Section 5. What's Next? Advanced Reporting

Appendix A – Brief Description of Wavecrest Products

Appendix B – Description of Reports—and Tips for Their Use

Appendix C – Product Usage Aids

Preface

Welcome to the Operator's Startup Guide! An "Operator" is a person who uses a Cyfin or CyBlock product to create, distribute, save and retrieve employee Web-use reports. We assume that you are—or soon will be—such a person.

This Guide is designed to:

- Familiarize you with the product and its Web-use reporting capabilities.
- Give you a foundation for more advanced usage of the product.

It includes five short *sections* and three relatively brief *appendices*.

Sections 1, 2 and 3 describe the products' reporting capabilities and the use of access control accounts.

Section 4 will help you create two of the product's sixteen reports. One of these is a summary-level report used for *screening* and overview purposes. The other is a detailed-level, drill-down report typically used in *investigations* of apparent abuse. In addition to giving you a little hands-on experience, the exercise will show you how these two reports can be used together very effectively.

Note. We assume that you or one of your colleagues have installed a Cyfin or CyBlock product at your location and have connected it to a source of logfiles. Logfiles provide the raw data needed for report generation.

Section 5 provides a brief introduction to the products' *advanced* reporting capabilities.

Finally, at the back of the Guide, you'll find three appendices. The first two provide more detail on Wavecrest products and on the reports they can produce. The last appendix tells you where you can quickly obtain additional information and help if you need it.

Note. *Sections 2, 3 and 4 contain the most essential information.* Sections 1 and 5 and the three appendices provide introductory and supplemental information that you may be able to skip.

Note for CyBlock Operators: Although CyBlock is designed to filter as well as report on Web-use, only CyBlock *administrators* can input or change filter settings. Consequently, because it's intended for *operators*, this Guide is devoted solely to reporting.

We hope you find our Guide helpful. Let us know if you have any comments or suggestions about it. And now, if you're ready, let's get started. Good luck!

1. Introduction

1.1. The Operator Concept.

As indicated in the Preface, Operators are persons like you who use Cyfin or CyBlock products—or soon *will* be using them—to create, modify, distribute, save, retrieve and use Web-use reports. You don't need to be an IT expert to be an operator. You only need to have an interest in—or have an assignment related to—management or control of Web-use in the workplace.

1.2. The Operator's Main Tool.

Aside from the Cyfin or CyBlock software itself, your main tool is the Web browser on your personal computer. (Typical browsers are Microsoft Internet Explorer and Netscape Navigator.) To create and retrieve reports, you simply enter a few simple instructions and view the resultant data on your browser. Operating a Cyfin or CyBlock product through your browser is quite easy. In fact, it's very similar to using various Internet or Web services with which you are probably already familiar. Some say it's as easy as "ordering a book on Amazon.com." Once again, the point is, you don't need any IT know-how to create and retrieve reports, although having it doesn't hurt.

1.3. Access Control Accounts.

To perform your operator functions easily and securely, you'll need an "Operator Account." If you don't have one yet, see your network or product administrator or other IT-responsible person. (Access control accounts are discussed in detail in Section 3.)

1.4. Purpose of this Guide.

With the above background in mind, and as touched on in the Preface, the basic purpose of this document is to familiarize you with the:

- Reporting capabilities of the product.
- Use of Operator Accounts (as distinguished from Administrator Accounts).
- Steps necessary to access the product and to create, distribute, save and retrieve reports.

To accomplish most of the last objective, i.e., creating reports, Section 4 of the Guide will lead you through a hands-on exercise to reinforce the "academic" knowledge that you gained in Sections 1, 2 and 3. During the exercise, you'll create and view two of the products' most-used reports. You'll also see how they work together to help you quickly pinpoint problem areas.

Note for CyBlock Operators: Although CyBlock is designed to filter as well as report on Web-use, only CyBlock *administrators* can input or change filter settings. Consequently, because this Guide is for operators, it is devoted solely to *reporting*.

1.5. Advanced Usage.

Upon completion of these familiarization steps, you'll be prepared to go on to more advanced usage of the product. For now though, you don't need to think about that. (Advanced usage is discussed briefly in Section 5. In addition, Appendix C at the end of this Guide can direct you to additional product usage aids.)

Now, let's see what kind of reporting capabilities Cyfin and CyBlock have.

2. Your Product's Reporting Capability: an Overview

2.1. General.

Cyfin and CyBlock products feature comprehensive, customizable Web-use reporting capabilities. These capabilities can support all types of organizational structures, corporate cultures, policy variations, report format preferences, report content preferences, and workforce types and sizes. The main purpose of these capabilities is to provide accurate information for both "quick-look" screening and individual investigations of workers' visits to Web sites. Such sites could be on the Internet and/or on intranets and extranets. (See paragraph 2.2 for definitions of screening and investigation.)

The products' sixteen reports are designed to provide answers to a variety of questions such as the following: "Which workers visited which Web sites? When did they do so? How many times did they do so? What types of content (by category) were they seeking? Was the activity "acceptable," i.e., in compliance with our usage policy? What was the impact on the network? etc., etc."

To answer these questions from different perspectives, you can set up the reports to:

- Depict Web-use activity during a period of time that you specify.
- Show activity by individual user, selected workgroup(s), or the entire enterprise.
- Flag abusive activity based on your own usage policy provisions.
- Run manually on an ad hoc basis—or automatically on a scheduled basis.
- Be delivered to selected recipients.

(**Note.** Later on, you may want to take a look at Appendix B. It contains a full description of all sixteen reports—along with tips for using them).

The information produced by these reports helps you and your management:

- Improve compliance with your Acceptable Use Policy (AUP).
- Increase workforce productivity.
- Avoid personnel-related litigation.
- Protect network and information security.
- Avoid negative public relations resulting from litigation.
- Avoid unnecessary labor, legal, and bandwidth costs.

Evaluating the Product? Some readers may be using this Guide in conjunction with a free trial (evaluation version) of the product. If you are, you can still fully test the product's Web-use monitoring and reporting features—using your own data—with one minor exception. (See Appendix A, paragraph A.2.3 for details.)

2.2. Using Reports for User Screening and Investigation Purposes.

Some of the Cyfin and CyBlock reports are top-level "overviews" or summaries designed for *screening* purposes, while others are detailed drill-down reports that are designed to support *investigation* efforts. "Screening" and "Investigations" are defined below.

Screening. Screening is a process that quickly identifies Web activity that *may* be inappropriate or unproductive. Generally speaking, screening involves analysis of an entire group's—or entire enterprise's—Web-use activity. The objective is to quickly identify instances or areas of suspect activity that *may* be inappropriate or non-productive.

Investigations. In general, an "investigation" is a focused follow-on to the discovery of suspect activity during the screening process. Although not always, investigations usually involve detailed analysis of an *individual* employee's Web activity. The primary objective of an investigation is to confirm or refute the findings of the screening process. If the findings are confirmed, the investigation is used to provide information and evidence to support any required follow-up action.

Some of the more common screening and investigation issues that Cyfin and CyBlock can address are summarized in paragraphs 2.2.1 and 2.2.2 below.

2.2.1. Issues that Lend Themselves to Screening.

As mentioned above, a number of Cyfin and CyBlock reports are summarized overviews of Web-use activity that are designed to aid the screening process. Some typical issues that lend themselves to screening are listed on the next page, starting with "Legal Liability." (Note. While the issues themselves are listed and defined, the selection and use of specific reports to help resolve them is not. That subject is a little beyond the scope of this familiarization Guide. Please note though that we have a slightly more advanced guide—also free—that provides specific tips for the choice and use of Wavecrest reports. It's titled "Web-use Screening and Investigation Guide." To access or acquire a copy, see Appendix C.)

Now, for some issues that lend themselves to the screening process.

- **Legal Liability.** Do any employees (or departments) appear to be engaging in Web activity that puts the organization at legal risk, e.g., visits to pornography sites? If so, who are the employees, what types of sites are they visiting, and how much of this activity is taking place?
- **Other Unacceptable or Inappropriate Activity.** Aside from "legal liability" activity, do any employees or departments appear to be engaging in other types of Web activity that our policy says is "unacceptable?" If so, who are they and what types of sites are they visiting, and how much of this activity is taking place?
- **Unacceptable vs. Acceptable Activity.** How does the level of acceptable activity compare to the level of unacceptable activity (for a particular group or for the entire enterprise)?
- **Most Active Visitors - By Category.** Who are the most active visitors to certain categories of sites, e.g., shopping, sports, news, finance, etc.?
- **Peak Periods - General.** What are the peak periods of Web-use activity, and how much of that activity is not related to business?
- **Email Problems.** Are any employees attempting to use Web email sites, e.g., hotmail.com? If so, who are they, which sites are they visiting, and how much of this activity is taking place?
- **Attempts to Visit Blocked Sites.** Which employees tried to access blocked sites? How extensive is this problem?
- **Intranet Usage.** To what extent are employees utilizing the intranet Web sites that were established—in part—for their benefit?

2.2.2. Issues that Lend Themselves to the Investigation Process.

Several Cyfin and CyBlock reports are designed to aid the *investigation* process. Known as drill-down reports, they are intended to cover a single employee. Typical issues that lend themselves to the use of drill-down reports for investigation purposes are listed below:

- **Abusive Activity.** An employee appears to be engaging in various types of "abusive" Web activity—as defined by your AUP. This would include all activity in Unacceptable categories and *may* include excessive activity in Acceptable and Neutral categories. Drill-down reports can answer the questions, "What types of sites—and which ones—is he or she visiting, and how much of this activity is he or she engaging in?"
- **Pornography.** An employee is suspected of visiting pornography sites. Which sites is he or she visiting, and how much of this activity is he or she engaging in?
- **Most Popular Sites.** Which Web sites does the employee mentioned above visit the most?
- **Attempts to Visit Blocked Sites.** An employee is suspected of attempting to visit blocked sites. Which sites is he or she visiting, and how much of this activity is he or she engaging in?

More Detail on Screening and Investigation. As mentioned earlier, another Guide, titled "Web-use Screening and Investigation Guide" goes into more detail on the use of Cyfin and CyBlock's reports to address the issues outlined above and more.

2.3. Correlating Policy and Product.

In addition to facilitating the screening and investigation processes discussed above, Cyfin and CyBlock can be customized to directly correlate with—and support—customers' Acceptable Use Policies (AUPs). Administrators customize the product by using its Advanced Settings to:

- Classify (rate) categories as "Acceptable," "Unacceptable," or "Neutral"
- Detect abuse (policy violations) automatically.
- Apply different policy rules to different workgroups if desired.
- Permit reporting on individual users, specific workgroups, or entire enterprises.
- Exclude designated individuals (e.g., "VIPs") from reports.
- Deliver "exception-only" reports.
- Add as many as 12 custom categories to the product's 60 standard categories. (Custom categories are ideal for tracking local intranet activity.)
- Schedule reports to run automatically.

We recommend that you coordinate closely with your Cyfin or CyBlock product administrator to:

- Take advantage of these advanced policy-support capabilities.
- Ensure that the reports you create reflect your organization's policy-compliance guidelines.
- Ensure that the reports you create reflect your organization's report-design and report-distribution preferences.

(**Note.** After going through the exercise in this Guide, you may want to learn more about tailoring the product to your policy. When you get to that point, see our document titled: "Planning Guide: Preparing to Implement a Web-use Monitoring Program.")

2.4. The Bottom Line?

Cyfin and CyBlock reports help enhance workforce productivity and ensure regulatory and policy compliance—while minimizing legal liability exposure and reducing labor, legal and bandwidth costs.

3. Your Operator Account

3.1. Access Control Accounts.

To use the capabilities discussed above, you'll need a special, partial-access "Operator Account." (And, as we said earlier, if you don't have one yet, see your network administrator or other IT-responsible person.)

Operator accounts are typically assigned to non-IT personnel such as HR representatives and business unit managers. Operators can access the product directly to create, distribute, save and retrieve reports as discussed in paragraph 3.2. However, they aren't permitted to make technical or product administration changes.

Note. Unlike Operator Accounts, Administrator Accounts let holders perform all operator functions plus all functions that deal with product setup and administration, including filtering if used. Smaller organizations may want to assign all operator and all administrator functions to one person. If so, they only need one administrator account. No operator accounts are needed. (For info on Administrator Accounts, see the Wavecrest document titled "Startup Guide for Administrators.")

3.2. Operator Account Authorization and Setup.

Typically, operator accounts will be authorized by management and set up by IT. Each account, including yours, will be authorized and set up to either:

- Generate reports that cover all Web users monitored by the product.
- Generate reports that are limited to a specified sub-set of users.

Examples of sub-sets could include (a) an operator's subordinate employees, or (b) a designated group of employees assigned to an HR representative for Web-use monitoring purposes.

Note. For security and administrative control purposes, operators will be issued (or will choose) usernames and passwords.

3.3. Accessing the Product.

As an authorized operator, you can access the product—and create and view reports—from your own desktop computer's Web browser. And you can do so without assistance from IT personnel. As the steps below indicate, the procedure is very simple. (You don't have to go through these steps right now, but it doesn't hurt to get familiar with them.)

- Enter the proper Web address URL into your Web browser (obtain from the product Administrator)
- Enter your username and password (obtain from the product Administrator)
- Click on desired action under the "Reports" menu.

You can then create, view, modify, schedule, and control the distribution of manual and scheduled reports by clicking on the appropriate menu and screen settings.

Note. If you like, your administrator can create a desktop shortcut for you to facilitate your access to the product. The administrator can also help with matters pertaining to your account, username, password and miscellaneous security issues.

4. First-Time Report Generation: a Hands-on Exercise

4.1. The Task.

Now that you've absorbed some background information, it's time for a little hands-on exercise. During the exercise, you'll create and view two of our most popular reports, i.e., Site Analysis and User Audit Detail. Although you *could* create them as scheduled reports to be run automatically, you won't be doing that. You'll be creating them as manual (ad hoc) reports that you can view almost immediately.

The Site Analysis Report is a summary-level overview. It's typically used as a high-level screening tool that lets you quickly identify areas of *possible* abuse or misuse. The User Audit Detail Report is a detailed, drill-down analysis that's typically used for follow-up investigations of an individual user's suspect activity.

Note. We chose these two particular reports to illustrate what Wavecrest calls the "screen-first, drill-down-second" approach. To ensure that this approach is demonstrated clearly, here's what we'll be asking you to do. While you're viewing the first report, i.e., Site Analysis, we'll ask you to note the ID of any one employee that exhibits substantial Web-use. Then, when you create the second report, you can run it against that same ID, for the same time period. Then, when you view *that* report, you'll see a highly detailed, expanded picture of that one employee's activity.

4.2. Getting Ready.

To get started you'll need a:

- Computer with network connectivity and Internet access—to reach Web sites.
- Web browser—to create, view and distribute reports.
- URL (Web site address)—to access the product.
- Username and password—for authentication.

You will also need to be sure that the product has been connected to its source of logfiles. And you'll need to know the period of time that is covered by these logfiles. If you need assistance with any of these five "prerequisites," please see your network administrator or other IT-responsible person.

A Note on Customization. The reporting capabilities of Wavecrest products can be customized in a variety of ways. Customization ensures that all reports reflect your organization's:

- Web-use policy provisions.
- Preferences for report content.
- Preferences for restrictions on user coverage.

Customization is done via several advanced features. Wavecrest sets these features at default values before downloading or shipping the product. To customize the product, your network administrator (or other IT-responsible person) must replace these defaults with settings that reflect your organization's policy provisions and report-design

preferences. Note. At this point in time, this customization may or may not have been done, but it doesn't really matter. If the logfile connection mentioned above has been made, you can create and run your reports with the defaults or with customized settings.

OK, if you're ready, let's get started on the exercise.

4.3. Creating a Site Analysis Report

General. The instructions below will help you create and run a basic Site Analysis report. The report will analyze, format and display historical Web-use data related to employees monitored by the product. Site Analysis is a comprehensive, summary-level report that identifies users, categorizes their activity by Web site content, shows the total visits for each user in each category, and rates the activity for "acceptability." It also provides useful bandwidth consumption data.

Please proceed as follows:

- Click on "Reports" at the top of the screen.
- Click on "Manual."
- Click on "Site Analysis."

This will open the three-section Reports – Manual - Site Analysis screen shown in figure 4-1 below.

Figure 4-1 Screen for Creating a Site Analysis Report

The settings in the screen are meant to be self-explanatory. However, if you need or want more detailed information on these settings, just click on the "quick reference" question mark at the top of the screen. To create and run your report, please refer to figure 4-1 and follow the instructions below.

A. Report Settings Section.

- **Report Delivery:** Do not disturb the default setting.
- **ID Type:** Do not disturb the default setting.
- **Thresholding:** Do not disturb the default setting.

Note. These settings can be changed for more advanced reporting, but we're not going to do that at this time.

B. Report Timeframe Section.

- **Start Date/Time:** Select the desired month, day and start time.
- **Stop Date/Time:** Select the desired month, day and stop time.

Note. Be sure to choose a time span that you know is in the logfile that is providing the raw data for your report. Check with your IT person if necessary. Also, to quickly verify that the proper data is displayed, do not select an excessively long time span.

C. Groups and IDs Section.

- **Selected Groups:** Ensure that this field reads "Enterprise." If it doesn't, just type it in.
(Note: With this field set to "Enterprise," your report will contain all active Internet users whose activity is recorded in the logfiles.)
- **Selected IDs:** Leave blank.

Now click "**Submit**" to start your report. When the progress meter reaches 100%, a popup with a hyperlink to your report will appear. Click on the hyperlink and the report will appear automatically in your browser. Scroll down and notice the amount of detail.

A Final Note. While viewing your report, look for an employee that had considerable Web-use activity. Make an offline note of the employee's ID. In the next part of this exercise, you'll be creating and viewing a drill-down report to see that particular employee's activity in much more detail.

4.4. Creating a User Audit Detail Report

General. The instructions below will help you create and run a basic User Audit Detail Report. The report will analyze, format and display Web-use data related to the user you identified in the Site Analysis report. The User Audit Detail report sorts the user's activity into content-labeled categories, shows the "acceptability" rating for each category, and identifies each visit separately. For each visit, the report shows URL (Web page address), time-of-visit, and download time.

Instructions. Please proceed as follows:

- Click on "Reports" at the top of the screen.
- Click on "Manual."
- Click on "User Audit Detail."

This will open the three-section Reports – Manual - User Audit Detail screen shown in figure 4-2 below.

The screenshot shows the 'Reports - Manual - User Audit Detail' interface. The 'Report Settings' section includes dropdown menus for 'Report Delivery' (set to 'Wait For Report'), 'ID Type' (set to 'Login Names'), 'Thresholding' (radio button for 'Disable' is selected), and 'Hits-Visits' (set to 'Visits Only (does not include jpg, gif, etc.)'). The 'Report Timeframe' section shows date and time inputs for 'Start Date/Time' (Aug 17, 2004, 12:00 A.M.) and 'Stop Date/Time' (Aug 24, 2004, 11:59 P.M.). The 'Groups and IDs' section features a 'Selected Groups' list containing 'Enterprise' and a 'Selected IDs' list with a search button. At the bottom are 'Submit' and 'Reset' buttons.

Figure 4-2 Screen for Creating a User Audit Detail Report

The settings in the screen are meant to be self-explanatory. However, if you'd like more detailed information on these settings, just click on the "quick reference" question mark at the top of the screen. Now, to create and run your report, please refer to figure 4-2 and follow the instructions below.

A. Report Settings Section.

- **Report Delivery:** Do not disturb the default setting.
- **ID Type:** Do not disturb the default setting.
- **Thresholding:** Do not disturb the default setting.

Note. These settings can be changed for more advanced reporting, but we're not going to do that at this time.

B. Report Timeframe Section.

- **Start Date/Time:** Enter the same month, day and start time you used for your Site Analysis Report.
- **Stop Date/Time:** Enter the same month, day and start time you used for your Site Analysis Report.

C. Groups and IDs Section.

- **Selected Groups:** Click on "Search" and find the group to which the employee is assigned. If you're not sure, choose "Ungrouped IDs." Highlight the group and click on "Submit."
- **Selected IDs:** Enter the ID of the employee you identified in the Site Analysis Report.

Now click "**Submit**" to start your report. When the progress meter reaches 100%, a popup with a hyperlink stating "All IDs" will appear. Click on the hyperlink and the report will appear automatically in your browser. Notice the amount of detail.

Congratulations! You've finished the exercise. Now you're ready to move on to more advanced reporting—as discussed briefly in Section 5.

5. What's Next? Advanced Reporting

Now that you've completed the exercises in Section 4, you're ready to work with your Cyfin or CyBlock Administrator to customize the product and its sixteen reports. We won't actually do that now, but here are some of the more advanced capabilities that you and your Administrator can take advantage of when you're ready to do so.

Policy-Support. You can use the product's optional policy-based features to support your organization's Acceptable Usage Policy. To do this simply:

- Classify categories as Acceptable, Unacceptable or Neutral to indicate acceptability
- Set "number-of-visit" thresholds in each category to automatically flag abuse.

User-Grouping. Users can be "grouped" in reports according to organizational assignment, work location or other attribute. This enables the product to report on Web usage for an individual user, selected departments, or an entire enterprise. This means that you can create and deliver individualized reports to selected recipients. For example, you can ensure that department managers who are authorized recipients receive reports that only cover their own employees. This gives them only the information they need while minimizing privacy issues. (For CyBlock, grouping also enables filtering rules to be set up differently for different groups if desired.)

"VIP" Exclusions. You can exclude selected individuals ("VIPs") from reporting and filtering processes. Once an ID is added to the VIP group, it will not appear on any reports (or be subjected to filtering if it's used).

Custom Categories. If you want, you can add custom categories to track employees' visits to Web sites of local or special interest. Examples include intranet sites, partner company sites, and highly specialized Internet sites that are unique to your organization's business or mission and may not be known to Wavecrest.

Report Formats. You can control the amount and type of information that appears in the product's reports, e.g., categories to be displayed or not displayed, number of visitors to be listed in reports, language to be used, etc.

Scheduling and Distributing Reports. You can set up specific reports to be scheduled for production at regular intervals and automatically delivered via email to specified recipients. Such reports can also be saved to disk.

These features and more can be accessed and customized by administrators via the product's main menu. If they need help, which they probably won't, screen tips for setting up each feature are available via the quick-reference "question mark" icon at the top right of each screen, and additional information is available under Help.

A. Appendix A — Brief Description of Wavecrest Products

A.1. Introduction

Designed to support a range of Web-use monitoring requirements and a variety of network infrastructures, Wavecrest products include:

- Cyfin, a family of reporting-only products
- CyBlock, a family of Web *filtering* products with built-in reporting capability.

All of these products are robust, customizable, and easy to use.

Note. CyBlock products' reporting capabilities are the same as Cyfin's. Consequently, they're only discussed once, in subsection A.2 immediately below. CyBlock's *filtering* capabilities will then be discussed separately in subsection A.3.

A.2. Cyfin and CyBlock Reporting Capabilities

All Wavecrest products have a number of identical reporting capabilities. They can all be used for numerous Web-use monitoring and management purposes. The associated features and some of the ways in which they can be used are discussed below.

A.2.1. Features.

Cyfin and CyBlock products have a robust set of features. A number of these are optional-use features. When all features are used, Cyfin and CyBlock products:

- Provide 16 different reports that can cover single users, specified workgroups, or a total enterprise.
- Identify Web users, determine *which* Web sites each user visited, count *how many times* they did so, and indicate *when* they did so.
- Show results in content-based categories, e.g., news, porn, chat, travel, etc.
- Provide summarized reports to support high-level screening of Web activity.
- Provide detailed, drill-down reports to support investigations of suspect Web activity.
- Let you rate each category (and thus each visit) as "Acceptable," "Unacceptable" or "Neutral" according to your own policies.
- Let you choose which categories to display in reports—if you don't want all of them to be visible.
- Let you set up custom categories and enter special URLs that are specific or unique to your business. Note that custom categories are excellent for tracking visits to intranet Web sites.
- Let you set up "number-of-visits" thresholds to automatically detect Web abuse on the basis of your own policy rules.
- Let you group users' activity by department or location.
- Can estimate the bandwidth consumed by each visit.
- Let you exclude VIP's Web-use activity from the product's reports.
- Let you specify time frames to be covered by reports.
- Let you run ad hoc manual reports in near-real time.

- Let you schedule reports to be run automatically at any chosen time.
- Let you distribute and save reports in a variety of ways.
- Let non-IT personnel (referred to as "operators") generate their own reports.

A.2.2. Using Wavecrest's Reports.

Management, HR, IT and legal personnel can use the information in Wavecrest reports to:

- Quickly screen large amounts of Web usage for suspect activity.
- Investigate suspected cases of Web abuse.
- Orient or re-orient employees in proper use of Web resources.
- Train or re-train employees in proper use of Web resources.
- Substantiate personnel actions such as discipline, termination, transfer, etc.
- Support the organization's position in any lawsuits.
- Monitor and improve intranet and extranet activities (via custom categories).
- Improve Web-enabled business processes.
- Fine-tune and improve the organization's AUP.
- Determine or change the sites or categories to be blocked.
- Revise network utilization and management "rules."
- Support or refute network expansion requirements.

For more information on how to use Wavecrest reports to maximum advantage, see Appendix B.

A.2.3. Evaluating the Product?

Some readers may be using this Guide in conjunction with a free trial of the product. If so, even though you're using an evaluation version of the product, you can fully test its Web-use monitoring and reporting features—using your own data. There is only one limitation, and it only applies to the four low-level (detailed audit) reports that display URLs:

- Top Web Sites
- User Audit Summary
- Category Audit Detail
- User Audit Detail

During evaluation, these reports will not display URLs in the following categories: Chat, Cults, Download Sites, Drugs, Email, Entertainment, Gambling, Games, Hate and Crime, Pornography, Public Proxy, Shopping. URLs in all other categories will be displayed.

NOTE: URLs in all categories can be viewed immediately after purchasing a software license.

A.3. Web-use Filtering Products

Like effective reporting products, useful filtering products need to be robust, flexible, scalable and easy to use. As discussed in this sub-section, *Wavecrest's CyBlock family of filtering products possesses these attributes*.

Note: Please note that Operator Accounts cannot be used to enter or change filter settings. Only persons with Administrator Accounts can do so. CyBlock *operators* should work closely with their CyBlock *Administrators* to coordinate filter setups.

A.3.1. CyBlock's Overall Capabilities.

CyBlock can be easily set up to block or allow access to *categories* of Web sites—and *individual* Web sites—that management considers inappropriate or unacceptable. Naturally, the definition of “inappropriate” and “unacceptable” will vary from organization to organization. However, *typical* examples of inappropriate or unacceptable sites are those that feature pornography, shopping, travel, chat, etc.

A.3.2. CyBlock Filtering Capabilities.

CyBlock is an advanced Web-use monitoring product that is both comprehensive and easy to use. Based on the customer’s policies and criteria, CyBlock can be set up easily to block Web-access activity that management deems inappropriate or unacceptable, e.g., visits to pornographic and other nonproductive Web sites. It can also be set up to allow activity that management deems appropriate. More specifically, CyBlock can be easily set up to:

- Block users’ access to selected *standard* categories of Web sites—while allowing access to all other categories.
- Block users’ access to selected *custom* categories of Web sites—while allowing access to all other categories.
- Implement “Permission Access”, i.e., allow users to access a special custom category containing selected URLs—while blocking access to all other categories.
- Block all (or selected) users from access to all Web sites
- Allow all (or selected) users to access all Web sites
- Add URLs to standard and custom categories.

CyBlock’s policy-support blocking actions can be applied uniformly (globally) to an entire organization, or they can be applied in unique ways to single users and/or specific workgroups.

Note that CyBlock’s 60 standard categories can be augmented with up to twelve custom categories. Custom categories let you block access to selected sites of local or special interest, i.e., sites related to highly specific issues that are unique to your organization.

B. Appendix B: Wavecrest Reports — Their Descriptions — and Tips for Their Use

B.1. Background

Wavecrest Computing's Cyfin and CyBlock products provide sixteen customizable Web-use activity reports. These reports are designed to answer a wide variety of Web-use management questions. For example:

- "Which users visited which Web sites, how often did they do so, when did they do so, and what type of content were they seeking?"
- "Is the content they were seeking acceptable under our AUP?"
- "How much unacceptable activity is taking place?"
- "Do any of the visits put the organization at legal liability risk?"
- "What impact is this activity having on the network?"
- "What impact is it having on workforce productivity?"

By answering these questions, the reports can:

- Show overall patterns of Web activity.
- Gauge compliance with the organization's AUP.
- Identify instances of suspected abuse.
- Provide accurate information to support related investigations and follow-on actions.

Wavecrest reports depict Web-use activity during a period of time specified by the report requestor. Additionally, most reports can show activity by individual user, selected workgroup(s), or the entire enterprise. And they can be configured to support a wide variety of organizational structures, corporate cultures, policy variations, report format and content preferences, and workforce types and sizes.

Wavecrest reports can be run manually on an ad hoc basis, or they can be set up to run automatically on a scheduled basis.

Three general types of reports are available:

- High-Level Screening Reports – Designed to support (1) Web-use screening, i.e., the effort to identify suspected cases of misuse or abuse, and (2) high-level analysis of Web-use activity, i.e., the effort to identify patterns of Web-use activity which may require adjustments to policies, processes and procedures.
- Detail Audit Reports – Designed primarily for drill-down purposes—to support detailed investigations of individual cases and to substantiate corrective actions.
- Supplemental Reports – Designed primarily to support network management and product administration.

All three types are discussed below.

B.2. High-Level Screening Reports

This section of the appendix describes "high level" Cyfin and CyBlock reports that are used primarily for macro-level, general screening purposes.

B.2.1. Site Analysis Report

Description. This is Wavecrest's most comprehensive and all-encompassing high-level screening report. For a selected user or group of users, or for an entire enterprise, it depicts Web site visits from a variety of perspectives. Perhaps the two most important are: (1) Total visits by classification (acceptable, unacceptable, neutral), and (2) Total visits by category (shopping, pornography, etc.). Other vital information is also included, e.g., most active categories, most active users, peak traffic hours graph, download volumes, etc. Individual users are listed in this report, but individual sites (URLs) are not.

Usage. The Site Analysis report can be used to gain a multi-perspective "big picture" view of Web-use activity engaged in by a single user, a group of users, or an entire enterprise. It is especially useful for identifying suspected problems in terms of excessive amounts of inappropriate, unproductive or unacceptable activity. This report can prompt specific audits and investigations using more detailed drill-down reports (see Detail Audit Reports, described later).

B.2.2. Legal Liability Report

Description. Displays only "Legal Liability" Web activity, i.e., visits to sites in the Cults, Drugs, Gambling, Hate and Crime, Pornography, and Public Proxy categories. Total visits are presented by category and by individual user. Individual sites (URLs) are not separately identified.

Usage. Gives managers and other responsible individuals a "quick-look" picture of any "legal liability" activity taking place. From this picture, they can quickly identify the individuals apparently engaging in such activity. This information can prompt more detailed individual audits and investigations, using more detailed drill-down reports (see Detail Audit Reports, described later).

B.2.3. All User Summary Report

Description. A tabularized report that depicts each user's activity from a high-level "acceptability" perspective. For each user, this report shows the total number of visits that have been classified as "Acceptable," "Unacceptable," and "Neutral." Extraneous hits (banner ads, audio, graphics, etc.) are not counted. All users are listed, but individual sites visited are not identified.

Usage. Presents management with a "quick-look" view of the number of acceptable, unacceptable and neutral visits made by each individual user. Responsible personnel can use the report for quick assessments of individual users' activity in terms of "acceptability." If the assessment is satisfactory, further review or investigation may not be warranted.

B.2.4. Acceptable Visit Report

Description. Depicts Web-use activity for categories classified as "Acceptable." It first provides an uncategorized total of such activity. Then, for each Acceptable category, it shows the total number of visits. Then, for each such category, the report lists the active users and shows the total number of visits that each made within that category. Users are listed in descending order according to number of visits. Other useful/related information is also provided, e.g., the percentage distribution of visits among the Acceptable categories. (**Note.** Users are identified but individual sites are not.)

Usage. Responsible recipients can quickly determine the amount and type of Acceptable activity. They can do this on an individual category or on a "grand total" summary basis for all Acceptable categories. They can also quickly identify the most active users of Web sites in Acceptable categories.

B.2.5. Unacceptable Visits Report

Description. Depicts only Web-use activity for categories classified as "Unacceptable." It first provides an uncategorized total of such activity. Then, for each Unacceptable category, it shows the total number of visits. Then, for each such category, the report lists the active users and shows the total number of visits that each made within that category. Users are listed in descending order according to number of visits. Other useful/related information is also provided, e.g., the percentage distribution of visits among the Acceptable categories. (**Note.** Users are identified but individual sites are not.)

Usage. Management can use this report to quickly assess the amount and type of Unacceptable activity and to identify users of Unacceptable sites, if any. This information can support "Management by Exception" techniques, i.e., if the results shown in this report are satisfactory, there may be no need for further analysis of activity that took place during the period covered by the report. On the other hand, if results are not satisfactory, drill-down reports such as Category Audit Summary and Category Audit Detail reports can be used to locate the source of the problem.

B.2.6. Neutral Visits Report

Description. Depicts only Web-use activity for categories classified as "Neutral." It first provides an uncategorized total of such activity. Then, for each Neutral category, it shows the total number of visits. Then, for each such category, the report lists the active users and shows the total number of visits that each made within that category. Other useful/related information is also provided. (**Note.** Users are identified but individual sites are not.)

Usage. Management can quickly determine the amount and type of "Neutral" activity. They can also identify the most active users of sites in the "Neutral" categories.

B.2.7. Denied Visits Report

Description. This report analyzes "denied visits" from several perspectives. First, at the highest level, it totals the visits in Acceptable, Unacceptable and Neutral categories. Then it shows total denied visits for each category. Then, to highlight the users who had the most denied visits, the report lists the users in descending order of the number of denied visits. Then, for each category, the report lists individual users who were denied access to Web sites or pages. For each such user, the report indicates the number of blocked or failed attempts. (Successful attempts are not shown). Individual users are identified but specific sites are not.

Note. "Denied" attempts to access a Web page can signify that (a) the user may not be authorized to receive the page, (b) the page may not have been found by the Web server, or (c) access to the page may have been blocked.

Usage. A significant number of denied visits can be an indicator of misuse or abuse of Web access. This screening report, along with others, can be used to identify possible instances of such. It can also be used to verify that Web-access filtering—if used—is working properly.

B.2.8. Custom Categories Report

Description. Can only be used if custom categories have been set up locally. If they have, the report:

- Identifies the users that visited Web sites in each custom category.
- Totals the visits made by each of those users within the category.

This report does not identify individual sites.

Usage. Using custom categories set up by the product user, this report focuses on subjects of local or specific interest to the enterprise. The information provided can help determine, for example, if employees are properly using intranet sites, Human Resources sites, supplier sites, customer sites, etc.

B.2.9. Top Web Sites Report

Description. A "most-popular-sites" report. For a reporting period that you select, it:

- Lists the Web sites (URLs) visited by a selected user or group — in descending order by the number of visits for each site.
- Indicates each site's category

Individual user IDs are not shown on this report unless the entire report only covers one user. If it covers only one user, the user ID is shown in the report's header. Hyperlinks to all visited Web sites are provided to facilitate further analysis.

Usage. "Highlights" the Web sites that were visited most by the selected user (or group of users) during the reporting period. Management can use it to quickly determine which sites are most popular with the user or group being reported on. They can then judge whether the "pattern" they see is satisfactory or not.

B.2.10. Category Audit Summary Report

Description. Focuses on a single category, e.g., pornography. It's designed to provide a *quick-look analysis* of the monitored users' visits to Web sites in that one category. It does this by presenting (a) a summarized total of all the visits in that category and (b) the sites the users have been visiting, listed in order of "popularity." This presents a clear, summarized view of all activity in the selected category—a view that can be extremely useful in terms of quickly determining if a *real* problem exists in a particular Web-access category. The report can be set up to include *all* users or a single selected group, but individual users are not identified. Additionally, in one setup session, you can (if you so desire) create multiple reports, with each report covering a different category.

Usage. Used for analyzing and determining the volume of activity in a single specified category. If the information tells you that a true problem may exist, you can drill down deeper and pinpoint the source by using a Category Audit Detail Report or a User Audit Detail Report.

B.3. Detail Audit Reports

This section of the appendix describes Cyfin's and CyBlock's drill-down reports. These reports are typically used for detailed investigation purposes.

B.3.1. User Audit Summary Report

Description. An investigation tool that focuses on a single user's activity. It lists all the Web sites (URLs) visited by the user during the reporting period, shows the total number of visits made to each of these sites, and indicates each listed site's category. A hyperlink to each site is provided to facilitate further review by management. (Note. Each site is only listed once, in descending order by number of visits. Multiple visits to the same site are not listed or time-stamped separately; for this level of detail, see User Audit Detail Report.)

Usage. Gives management a listing of every site the user visited during the selected time frame. It is most useful during follow-up investigations of suspected misuse or abuse of Web access privileges. It can also be used for personnel appraisal and counseling purposes and to support disciplinary actions, including termination.

B.3.2. User Audit Detail Report

Description. A highly detailed investigation tool. Like the User Audit Summary, it focuses on a single user's activity, but in more depth. It starts by presenting summary-level totals of visits by category and acceptability. It then lists every visit separately in chronological order by date and time. For every visit, it shows the site's category and full URL.

Usage. This report gives management a complete analysis of every visit the user made during the selected time frame. Highly detailed, it can be used to assess in depth the type, volume and timing of acceptable and unacceptable activity. It is most useful during follow-up investigations of suspected misuse or abuse of Web access privileges, but it can also be used for personnel appraisal and counseling purposes and to support disciplinary actions, including termination.

B.3.3. Category Audit Detail Report

Description. This report shows Web-use activity in one selected category, e.g., pornography, sports, shopping, etc. You select the report's category and time frame, and you specify whether you want to see "visits only" or "all hits," i.e., all URLs. You also set up the report to cover a single user, a particular group, or all the users in your organization. In addition to showing total Acceptable and Unacceptable activity and total download time, the report lists all of the covered user(s) who were active in that category during the selected time frame. For each listed user, the report shows each visit (or hit) separately, indicating its Web address (URL) and the time of occurrence. (**Note.** In a single setup session, if you want, you can create multiple reports, with each report covering a single category.)

Usage. Presents a clear and complete view of all activity in the selected category. It does this from several different perspectives. For example, if the category has been rated as "unacceptable," you'll be able to see: (a) all the users that have been engaging in the unacceptable activity, (b) the level of that activity, and (c) the sites and pages they have been visiting. Such information can be extremely useful in terms of gauging the exact extent and precise source(s) of a problem area.

B.4. Supplemental Reports

This section of the appendix describes Cyfin's and CyBlock's reports that are designed primarily to support network management and product administration.

B.4.1. Network Information Report

Usage. Helps Network Administrators manage bandwidth utilization. It can show them which categories and which times of day are the busiest or the most troublesome.

B.4.2. Site Analysis Bandwidth Report

Description. Presents a multi-faceted analysis of the bandwidth consumed during a time frame which you choose. The bandwidth consumed is broken down and presented from five different perspectives: overall acceptability, category breakdown, user, acceptability by user, and hourly consumption. The report can be set up to cover a single user, a selected group of users, or all users in the enterprise.

Usage. Helps administrators analyze bandwidth consumption from several perspectives. That is, it can indicate who is using the bandwidth, when they are using it, and for what purpose. If analysis reveals a problem, the report can also help pinpoint the source(s).

B.4.3. Top Non-Categorized Sites Report

Description. A highly useful "results-enhancement" tool. This report shows all unidentified activity, including the URLs of visits that the product was not able to categorize by content. The product places such activity in the "Other" category. For each URL listed, the report shows the number of hits and the full domain name. Individual user IDs are not shown. The list is sorted in descending numerical order by number of hits. Hyperlinks to all Web sites are also provided.

Usage. Useful to an administrator in at least two ways. (1) Among other advantages, the report identifies intranet and other special sites of local interest that have not previously been categorized and incorporated into the product's control list. To quickly resolve this issue, the administrator can create custom categories and populate them with the identified sites' URLs. (2) Administrators can also use this report to help improve *overall* across-the-board reporting results. That is, if they send a copy to Wavecrest, the company's list technicians will identify, research and categorize many of the unidentified "Other" URLs and incorporate them into the Wavecrest URL List. Either or both of these actions will help improve the coverage and usefulness of future reports.

C. Appendix C: Product Usage Aids

General. Cyfin Reporter is very easy to use. However, if you should need any help, the resources listed below are available to assist you. These resources are in addition to technical support services such as trouble-shooting assistance, product upgrades and categorization list updates.

C.1. Product Usage Guides

Operator's Startup Guide. A short but informative user's manual for newly appointed operators. Provides basic familiarization information and guides the operator through creation of two actual reports. Also discusses Operator Accounts and how to use them.

Introduction to Web-use Management and Monitoring. A basic but informative discussion of policy-based Web-use management and monitoring projects.

Web-use Screening and Investigation Guide. Describes the product's 16 reports and discusses how to use them for both high-level screening and drill-down investigation purposes.

Planning Guide: Preparing to Implement a Web-use Monitoring Program. Provides recommendations related to planning and preparing for implementation of a policy-based Web-use management and monitoring program.

Administrator's Startup Guide. A short but informative user's manual for newly appointed product administrators. Provides product familiarization information and guides the administrator through initial setup and configuration of the product. Also, briefly discusses Operator and Administrator Accounts and provides instruction on how to establish and use them.

C.2. "In-Product" Usage Aids (Built into Wavecrest products for on-screen viewing)

Quick Start Guide. Guides administrators and evaluators through basic product setup and usage steps.

Quick-Reference Screen Tips. Context-sensitive help instructions for using the product's screens.

Help/Documentation. Links to a variety of helpful documents and our Web site.

C.3. Product Usage Services

C.3.1. "OtherWise" Program (One-on-one Categorization Support)

A voluntary, confidential, no-charge service that helps categorize Web activity unique to your particular organization. Such activity includes employees' visits to intranet and other sites of interest to your organization only. Without a service like OtherWise, such sites may not be categorized in the normal reporting process. We encourage all customers to take advantage of this free service; it's guaranteed to increase your "categorization rate," i.e., the percentage of your organization's Web activity that is successfully categorized.

C.3.2. Product Usage Consultation.

Wavecrest offers a range of product usage consultation and training services to help customers get the most out of our products.

- **Telephone and Email - Based Support**

Technical and customer support representatives are available to answer questions about product set-up, policy support, technical issues and more — via phone or email at no cost.

- **Online Training for Administrators**

Cyfin or CyBlock administrators requiring more in-depth product consultation or support can meet one-on-one with a technical support specialist in Wavecrest's online meeting center. Schedule a meeting, login to Wavecrest's Macromedia® Breeze® Web conferencing center and you'll be able to ask questions and follow solution steps as they are demonstrated live, onscreen. These interactive, how-to sessions are ideal for administrators looking for additional training or assistance with anything from product set-up and configuration to scheduling and running reports. To schedule a training session or request pricing information, contact sales@wavecrest.net.

- **Online Training for Operators**

Cyfin or CyBlock operators can take advantage of Wavecrest's online conference center to quickly learn how to request and read Wavecrest's reports as part an effective Web-use management program. Simply login to Wavecrest's Macromedia® Breeze® Web conferencing center and you'll be able to ask questions and follow solution steps as they are demonstrated live, onscreen. Topics of special interest to operators include Acceptable Use Policy (AUP) support, generating and interpreting reports, and techniques for investigating incidents of Web abuse. To schedule a training session or request pricing information, contact sales@wavecrest.net.

C.4. Web Site Resources (Available at any time at no charge)

C.4.1. Advanced Features Description.

A description of Cyfin's advanced features with instructions on how to set them up and use them.

C.4.2. White Papers and Case Studies.

A number of informative papers that discuss Web-use management and monitoring.

C.4.3. Product Specifications and Feature Lists.

Functional and technical information for product users and administrators.

C.4.4. Support Forum.

An open online forum for customers to ask product-relevant questions, get answers, make suggestions, etc. at <http://forum.wavecrest.net>